SEL

NATIONAL BUREAU OF STANDARDS REPORT

1492

ON CERTAIN CHARACTER MATRICES

by

D. H. Lehmer

National Bureau of Standards, Los Angeles, California

NBS

U. S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS

U. S. DEPARTMENT OF COMMERCE
Charles Sawyer, Secretary

NATIONAL BUREAU OF STANDARDS
A. V. Astin, Acting Director

THE NATIONAL BUREAU OF STANDARDS

The scope of activities of the National Bureau of Standards is suggested in the following listing of the divisions and sections engaged in technical work. In general, each section is engaged in specialized research, development, and engineering in the field indicated by its title. A brief description of the activities, and of the resultant reports and publications, appears on the inside of the back cover of this report.

1. **ELECTRICITY.** Resistance Measurements. Inductance and Capacitance. Electrical Instruments. Magnetic Measurements. Electrochemistry.
2. **OPTICS AND METROLOGY.** Photometry and Colorimetry. Optical Instruments. Photographic Technology. Length. Gage.
3. **HEAT AND POWER.** Temperature Measurements. Thermodynamics. Cryogenics. Engines and Lubrication. Engine Fuels.
4. **ATOMIC AND RADIATION PHYSICS.** Spectroscopy. Radiometry. Mass Spectrometry. Physical Electronics. Electron Physics. Atomic Physics. Neutron Measurements. Nuclear Physics. Radioactivity. X-Rays. Betatron. Nucleonic Instrumentation. Radiological Equipment. Atomic Energy Commission Instruments Branch.
5. **CHEMISTRY.** Organic Coatings. Surface Chemistry. Organic Chemistry. Analytical Chemistry. Inorganic Chemistry. Electrodeposition. Gas Chemistry. Physical Chemistry. Thermochemistry. Spectrochemistry. Pure Substances.
6. **MECHANICS.** Sound. Mechanical Instruments. Aerodynamics. Engineering Mechanics. Hydraulics. Mass. Capacity, Density, and Fluid Meters.
7. **ORGANIC AND FIBROUS MATERIALS.** Rubber. Textiles. Paper. Leather. Testing and Specifications. Organic Plastics. Dental Research.
8. **METALLURGY.** Thermal Metallurgy. Chemical Metallurgy. Mechanical Metallurgy. Corrosion.
9. **MINERAL PRODUCTS.** Porcelain and Pottery. Glass. Refractories. Enameled Metals. Building Stone. Concreting Materials. Constitution and Microstructure. Chemistry of Mineral Products.
10. **BUILDING TECHNOLOGY.** Structural Engineering. Fire Protection. Heating and Air Conditioning. Exterior and Interior Coverings. Codes and Specifications.
11. **APPLIED MATHEMATICS.** Numerical Analysis. Computation. Statistical Engineering. Machine Development.
12. **ELECTRONICS.** Engineering Electronics. Electron Tubes. Electronic Computers. Electronic Instrumentation.
13. **ORDNANCE DEVELOPMENT.** Mechanical Research and Development. Electromechanical Fuzes. Technical Services. Missile Fuzing Research. Missile Fuzing Development. Projectile Fuzes. Ordnance Components. Ordnance Tests. Ordnance Research.
14. **RADIO PROPAGATION.** Upper Atmosphere Research. Ionospheric Research. Regular Propagation Services. Frequency Utilization Research. Tropospheric Propagation Research. High Frequency Standards. Microwave Standards.
15. **MISSILE DEVELOPMENT.** Missile Engineering. Missile Dynamics. Missile Intelligence. Missile Instrumentation. Technical Services. Combustion.

NBS PROJECT
1101-11-5100

February 14, 1952

NBS REPORT
1492

ON CERTAIN CHARACTER MATRICES*

by

D. H. Lehmer
National Bureau of Standards, Los Angeles, California

NBS

PREPRINT

*The preparation of this paper was sponsored (in part) by the Office of Naval Research

NBS No. 1492
2-14-52
PREPRINT

On Certain Character Matrices*

by

D. H. Lehmer

National Bureau of Standards, Los Angeles, California

For only a very limited class of matrices M is it possible to give explicit formulas for the determinant of M, the general element of M^k, the characteristic roots of M and the inverse of M. Non-trivial instances of such matrices are useful as examples in testing the correctness and efficacy of various matrix computing routines especially when the elements of the matrices are exact integers or rational numbers. The purpose of this note is to indicate a new set of such matrices. Although they arose in connection with a class of exponential sums, they appear to warrant an independent treatment. A discussion of the most general case will not be attempted here. The matrices considered are real and symmetric and of order p-1 where p is an odd prime.

The elements of our matrices are equal to 0, 1 or -1 and are based on what are called real non-principal characters modulo p. These are, for the cases considered, Legendre's symbols for which we use the notation [1]

$$\chi(a) = \left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } a \\ -1 & \text{if the congruence } x^2 \equiv a \pmod{p} \text{ is impossible} \\ +1 & \text{otherwise} \end{cases}$$

*The preparation of this paper was sponsored (in part) by the Office of Naval Research.

For example if $p = 7$ we have

a	0	1	2	3	4	5	6
$\chi(a)$	0	1	1	-1	1	-1	-1

Besides the simple properties

$$\chi(a)\ \chi(b) = \chi(ab)$$
$$\chi(a+p) = \chi(a)$$

we use the following identities

(1) $$\sum_{k=1}^{p-1} \chi(a+k) = -\chi(a)$$

(2) $$\sum_{k=1}^{p-1} \chi(a+k)\ \chi(b+k) = p\,\delta_a^{\ b} - 1 - \chi(a)\ \chi(b)$$

where $\delta_a^{\ b}$ is Kronecker's delta modulo p, that is

$$\delta_a^{\ b} = \begin{cases} 1 & a \equiv b \pmod p \\ 0 & a \not\equiv b \pmod p \end{cases} .$$

The first of these identities is equivalent to the well known fact that there is a residue for every non-residue modulo p. The second identity may be written

$$\sum_{k=0}^{p-1} \chi(a+k)\ \chi(b+k) = p\,\delta_a^{\ b} - 1 .$$

This is obvious if $a \equiv b \pmod p$ since $\chi^2(a+k) = 0$ or 1 according as $a + k$ is divisible by p or not. If $a \not\equiv b \pmod p$ we may

set $b - a \equiv r \pmod{p}$ and write the left side as follows

$$\sum_{k=0}^{p-1} \chi(a+k)\ \chi(b+k) = \sum_{h=0}^{p-1} \chi(h)\ \chi(r+h) \quad .$$

If we denote this sum by $S(r)$ and write

$$h \equiv rm \pmod{p}$$

we have

$$S(r) = \sum_{m=0}^{p-1} \chi(rm)\ \chi(rm+r)$$

$$= \chi^2(r) \sum_{m=0}^{p-1} \chi(m)\ \chi(1+m) = S(1) \quad .$$

Hence to show that $S(r) = -1$ we have only to show that

$$\sum_{r=1}^{p-1} S(r) = 1 - p \quad .$$

Now

$$\sum_{r=1}^{p-1} S(r) = \sum_{r=1}^{p-1} \sum_{h=0}^{p-1} \chi(h)\ \chi(r+h)$$

$$= \sum_{h=0}^{p-1} \chi(h) \sum_{r=1}^{p-1} \chi(r+h)$$

$$= - \sum_{h=0}^{p-1} \chi^2(h) = -(p-1)$$

by (1). This proves (2) in all cases. This identity appears to be due to E. Jacobsthal [2].

With these preliminaries we proceed to introduce our general matrix and to give its properties.

Let α be any integer parameter and let M_α be the square matrix of order p-1 whose general element a_{ij} is $\chi(\alpha+i+j)$, then:

I. The inverse M_α^{-1} has for its general element

$$a_{ij}^{(-1)} = \left\{\chi(\alpha+i+j) - \chi(\alpha+i) - \chi(\alpha+j) + \chi(\alpha)\right\}/p .$$

II. The characteristic equation

$$|\lambda I - M_\alpha| = 0$$

of M_α is $(\lambda^2-p)^{\frac{p-3}{2}}(\lambda^2+\chi(\alpha)\lambda-1) = 0$.

III. The determinant of M_α is $-(-p)^{(p-3)/2}$.

The result III follows at once from II by setting $\lambda = 0$. The result I, once guessed, may be verified as follows. We have to show that

$$\sum_{k=1}^{p-1} a_{ik}\, a_{kj}^{(-1)} = \delta_i^j \quad .$$

Substituting, we have

$$p^{-1}\sum_{k=1}^{p-1} \chi(\alpha+i+k)\left\{\chi(\alpha+k+j) - \chi(\alpha+k) - \chi(\alpha+j) + \chi(\alpha)\right\}$$

$$= p^{-1}[p\,\delta_i^j - 1 - \chi(\alpha+i)\,\chi(\alpha+j) - p\,\delta_{\alpha+i}^{\alpha} + 1 + \chi(\alpha+i)\,\chi(\alpha)$$

$$- \left\{\chi(\alpha+j) - \chi(\alpha)\right\}(-\chi(\alpha+i))]$$

by (1) and (2). Since $i \not\equiv 0 \pmod p$ the above expression reduces δ_i^j as required.

It remains to prove II. The method of proof given below is not the most direct one that could be given.[1] It has the merit, however, of producing as a byproduct the general element of any power of M_α and this information may be useful in checking routine computations of powers of a given matrix.

If we denote by $a_{ij}^{(k)}$ the general element of M^k we have

$$p\,a_{ij}^{(-1)} = \chi(\alpha+i+j) - \chi(\alpha+i) - \chi(\alpha+j) + \chi(\alpha)$$

$$a_{ij}^{(0)} = \delta_i^j$$

$$a_{ij}^{(1)} = \chi(\alpha+i+j)$$

$$a_{ij}^{(2)} = p\,\delta_i^j - \chi(\alpha+i)\,\chi(\alpha+j) - 1$$

the last result following directly from (2). An inspection of even this small sample of $a_{ij}^{(k)}$ together with considerations of symmetry leads one to the conclusion that $a_{ij}^{(k)}$ depends somewhat on the parity of k and that in making an inductive proof of the general form of $a_{ij}^{(k)}$ one should assume that

$$(3)\quad a_{ij}^{(k)} = \Psi_k(i,j) + S_k[\chi(\alpha+i) + \chi(\alpha+j)] + P_k\,\chi(\alpha+i)\,\chi(\alpha+j) + C_k$$

where S_k P_k C_k depend on α and p only and

$$\Psi_k(i,j) = \begin{cases} p^{k/2}\,\delta_i^j & \text{if } k \text{ is even} \\ p^{(k-1)/2}\,\chi(\alpha+i+j) & \text{if } k \text{ is odd}. \end{cases}$$

[1]An alternative short method of proof was suggested by R. M. Robinson.

At least, (3) is seen to hold for $k = -1, 0, 1, 2$ and we have in fact

$$(4) \qquad \begin{aligned} S_0 &= 0 & P_0 &= 0 & C_0 &= 0 \\ S_1 &= 0 & P_1 &= 0 & C_1 &= 0 \\ S_2 &= 0 & P_2 &= -1 & C_2 &= -1 \; . \end{aligned}$$

That $a_{ij}^{(k)}$ has the form (3) follows at once from (1) and (2) and, moreover, these latter identities give us recurrence relations for the S_k P_k and C_k. In fact if we assume that (3) holds for $k = 2m$ and if we substitute into the relation

$$a_{ij}^{(2m+1)} = \sum_{r=1}^{p-1} a_{ir}\, a_{rj}^{(2m)}$$

we find

$$(5) \qquad \begin{aligned} S_{2m+1} &= -P_{2m} = -\chi(\alpha)\, S_{2m} - C_{2m} \\ P_{2m+1} &= -S_{2m} - \chi(\alpha)\, P_{2m} \\ C_{2m+1} &= -S_{2m} \; . \end{aligned}$$

Similarly we find

$$(6) \qquad \begin{aligned} S_{2m+2} &= -\chi(\alpha)\, S_{2m+1} - C_{2m+1} = -P_{2m+1} \\ P_{2m+2} &= -p^m - S_{2m+1} - \chi(\alpha)\, P_{2m+1} \\ C_{2m+2} &= -p^m - S_{2m+1} \; . \end{aligned}$$

We have only to solve these difference equations for S_k, P_k, C_k subject to the initial condition (4).

The case of $\chi(\alpha) = 0$ is much simpler than $\chi(\alpha) = \pm 1$. In fact the above relations then become simply

$$-S_{k+1} = C_k = P_k$$

$$C_{2m+1} = C_{2m-1}$$

$$C_{2m} = -p^m + C_{2m} \quad .$$

The solution is easily seen to be

$$S_{2m} = 0 \qquad P_{2m} = C_{2m} = -(p^m - 1)/(p-1)$$

$$S_{2m+1} = (p^m - 1)/(p-1) \qquad P_{2m+1} = C_{2m+1} = 0 \quad .$$

Hence if

$$a_{ij} = \chi(i+j)$$

then

$$a_{ij}^{(2m)} = p^m \delta_i^{\,j} - \frac{p^m - 1}{p-1}\left\{\chi(ij) + 1\right\} \tag{7}$$

$$a_{ij}^{(2m+1)} = p^m \chi(i+j) + \frac{p^m - 1}{p-1}\left\{\chi(i) + \chi(j)\right\} \quad . \tag{8}$$

In case $\chi(\alpha) \neq 0$ the solution of the systems (5) and (6) involves the Fibonacci numbers

$$U_n = (A^n - B^n)/(A - B)$$

where

$$A = \tfrac{1}{2}(1 + \sqrt{5}) \; , \quad B = \tfrac{1}{2}(1 - \sqrt{5}) \quad .$$

Early values of U_n are given by the following table

n	-2	-1	0	1	2	3	4	5	6	7	8
U_n	-1	1	0	1	1	2	3	5	8	13	21

and in general

$$U_{n+1} = U_n + U_{n-1} .$$

In what follows we shall need to refer also to the companion sequence

(9) $$V_n = A^n + B^n = U_{n+1} + U_{n-1} .$$

The solution of (5) and (6) may be given as follows

$$S_k = - P_{k-1}$$

(10)
$$P_{2m+1} = \chi(\alpha) \left\{ p^{m+1} - p\, U_{2m+2} + U_{2m} \right\} / (p^2 - 3p + 1)$$
$$C_{2m+1} = \chi(\alpha) \left\{ p^{m} - p\, U_{2m} + U_{2m-2} \right\} / (p^2 - 3p + 1)$$

(11)
$$P_{2m} = - \left\{ p^{m+1} - p^m - p\, U_{2m+1} + U_{2m-1} \right\} / (p^2 - 3p + 1)$$
$$C_{2m} = - \left\{ p^{m+1} - 2p^m - p\, U_{2m-1} + U_{2m-3} \right\} / (p^2 - 3p + 1) .$$

The fact that these values satisfy the difference equations (5), (6) and the initial conditions (4) may be verified without using anything more complicated than the fact that

$$U_n = 3U_{n-2} - U_{n-4} .$$

Of course the expressions (10) and (11) are polynomials in p.

If (10) and (11) are substituted into (3) we obtain expressions for $a_{ij}^{(2m)}$ and $a_{ij}^{(2m+1)}$.

For example

$$(12)\quad \begin{aligned} a_{ij}^{(5)} &= p^2\, \chi(\alpha+i+j) + (p+2)\left\{\chi(\alpha+i) + \chi(\alpha+j)\right\} \\ &\quad + (p+3)\, \chi(\alpha)\, \chi(\alpha+i)\, \chi(\alpha+j) + \chi(\alpha) . \end{aligned}$$

We note that this does not become (8), with $m = 2$, if we set $\alpha = 0$. We now consider the trace of $M_\alpha^{\ k}$, that is the sum $\Sigma_{j=1}^{p-1}\, a_{jj}^{(k)}$ which is also the sum of the k-th powers of the characteristic roots of M_α. The case of $\chi(\alpha) = 0$ is simple. From (7) and (8) we have

$$\sum_{j=1}^{p-1} a_{jj}^{(2m)} = (p-1)\, p^m - 2(p^m-1) = (p-3)\, p^m + 2$$

$$\sum_{j=1}^{p-1} a_{jj}^{(2m+1)} = 0 .$$

Hence in both cases

$$\Sigma\, a_{jj}^{(k)} = \frac{p-3}{2}\,(p^{\frac{1}{2}})^k + \frac{p-3}{2}\,(-p^{\frac{1}{2}})^k + (-1)^k + 1^k .$$

Since this holds for $k = 1, 2, 3, \cdots$ the characteristic roots of M_0 must be those of the equation

$$(13)\qquad (\lambda^2 - p)^{(p-3)/2}(\lambda^2 - 1) = 0 .$$

This proves II in case $\chi(\alpha) = 0$.

For $\chi(\alpha) \neq 0$ we find from (3)

$$\sum_{j=1}^{p-1} a_{jj}^{(2m)} = (p-1)\, p^m - 2\,\chi(a)\, S_{2m} + (p-2)\, P_{2m} + (p-1)\, C_{2m}$$

$$\sum_{j=1}^{p-1} a_{jj}^{(2m+1)} = -\,\chi(a) p^m - 2\,\chi(a) S_{2m+1} + (p-2) P_{2m+1} + (p-1) C_{2m+1} .$$

If we substitute from (10) and (11) and simplify we obtain

$$\sum_{j=1}^{p-1} a_{jj}^{(2m)} = (p-3)p^m + U_{2m+1} + U_{2m+1}$$

$$= (p-3)p^m + V_{2m}$$

$$\sum_{j=1}^{p-1} a_{jj}^{(2m+1)} = -\chi(\alpha)(U_{2m+2} + U_{2m})$$

$$= -\chi(\alpha)\, V_{2m+1} \text{ .}$$

Recalling the definition (9) of V_n we may write in general

$$\sum_{j=1}^{p-1} a_{jj}^{(k)} = \tfrac{1}{2}(p-3)(p^{\frac{1}{2}})^k + \tfrac{1}{2}(p-3)(-p^{\frac{1}{2}})^k + (-\chi(\alpha)A)^k + (-\chi(\alpha)B)^k \text{ .}$$

This shows that the characteristic roots of M_α consist of $\frac{1}{2}(p-3)$ roots $p^{\frac{1}{2}}$, $\frac{1}{2}(p-3)$ roots $-p^{\frac{1}{2}}$, $-\chi(\alpha)A$ and $-\chi(\alpha)B$. Since

$$A + B = 1 \text{ ,} \quad AB = -1 \text{ ,}$$

the characteristic equation of M_α is

$$(\lambda^2 - p)^{(p-3)/2}(\lambda^2 + \chi(\alpha)\lambda - 1) = 0 \text{ .}$$

Although this was derived on the assumption that $\chi(\alpha) \neq 0$, if we set $\chi(\alpha) = 0$ we do obtain (13). This completes the proof of II.

Concerning the latent vectors of M_α, the reader may verify that, corresponding to a root ρ of

$$\lambda^2 + \chi(\alpha)\lambda - 1 = 0$$

there is the latent vector whose j-th component is

$$\chi(\alpha + j) - \chi(\alpha) - \rho \;.$$

The following example will illustrate the foregoing. We take $p = 7$, $\alpha = 3$; then our matrix M_3 is

$$M_3 = \begin{pmatrix} -1 & -1 & 0 & 1 & 1 & -1 \\ -1 & 0 & 1 & 1 & -1 & 1 \\ 0 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 0 \\ -1 & 1 & -1 & -1 & 0 & 1 \end{pmatrix}$$

whose determinant is -49. If the elements of M^{-1} are each multiplied by 7 we obtain

$$\begin{pmatrix} -4 & -2 & -1 & -1 & -2 & -4 \\ -2 & 1 & 2 & 1 & -2 & 0 \\ -1 & 2 & 2 & -1 & 0 & -2 \\ -1 & 1 & -1 & 0 & -3 & -3 \\ -2 & -2 & 0 & -3 & -4 & -3 \\ -4 & 0 & -2 & -3 & -3 & -2 \end{pmatrix}$$

By (12) we have, for example,

$$M_3^5 = \begin{pmatrix} -42 & -40 & 9 & 57 & 56 & -42 \\ -40 & -29 & 20 & 39 & -40 & 58 \\ 9 & 20 & 20 & -59 & 58 & -40 \\ 57 & 39 & -59 & 48 & -41 & -41 \\ 56 & -40 & 58 & -41 & -42 & 7 \\ -42 & 58 & -40 & -41 & 7 & 56 \end{pmatrix}$$

February 26, 1952.

References

[1] See for example E. Landau, Elementare Zahlentheorie New York, Chelsea, 1946, p. 83-87.

[2] E. Jacobstahl, "Über die Darstellung der Primzahlen der Form 4n + 1 als Summe zweier Quadrate," Jour. für. Math. v. 132, 1907, pp. 238-245.

THE NATIONAL BUREAU OF STANDARDS

Functions and Activities

The National Bureau of Standards is the principal agency of the Federal Government for fundamental and applied research in physics, mathematics, chemistry, and engineering. Its activities range from the determination of physical constants and properties of materials, the development and maintenance of the national standards of measurement in the physical sciences, and the development of methods and instruments of measurement, to the development of special devices for the military and civilian agencies of the Government. The work includes basic and applied research, development, engineering, instrumentation, testing, evaluation, calibration services, and various scientific and technical advisory services. A major portion of the NBS work is performed for other government agencies, particularly the Department of Defense and the Atomic Energy Commission. The functions of the National Bureau of Standards are set forth in the Act of Congress, March 3, 1901, as amended by Congress in Public Law 619, 1950. The scope of activities is suggested in the listing of divisions and sections on the inside of the front cover.

Reports and Publications

The results of the Bureau's work take the form of either actual equipment and devices or published papers and reports. Reports are issued to the sponsoring agency of a particular project or program. Published papers appear either in the Bureau's own series of publications or in the journals of professional and scientific societies. The Bureau itself publishes three monthly periodicals, available from the Government Printing Office: the Journal of Research, which presents complete papers reporting technical investigations; the Technical News Bulletin, which presents summary and preliminary reports on work in progress; and Basic Radio Propagation Predictions, which provides data for determining the best frequencies to use for radio communications throughout the world. There are also five series of nonperiodical publications: the Applied Mathematics Series, Circulars, Handbooks, Building Materials and Structures Reports, and Miscellaneous Publications.

Information on the Bureau's publications can be found in NBS Circular 460, Publications of the National Bureau of Standards ($1.00). Information on calibration services and fees can be found in NBS Circular 483, Testing by the National Bureau of Standards (25 cents). Both are available from the Government Printing Office. Inquiries regarding the Bureau's reports and publications should be addressed to the Office of Scientific Publications, National Bureau of Standards, Washington 25, D. C.

NBS